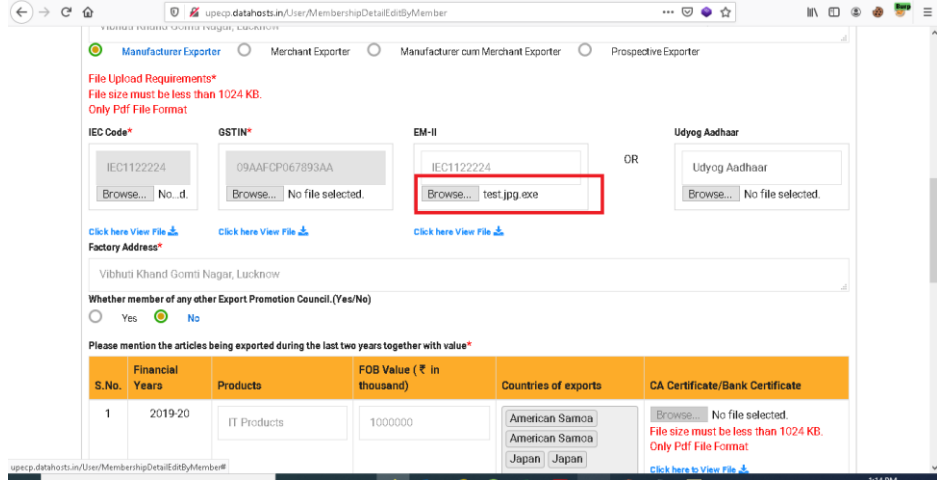
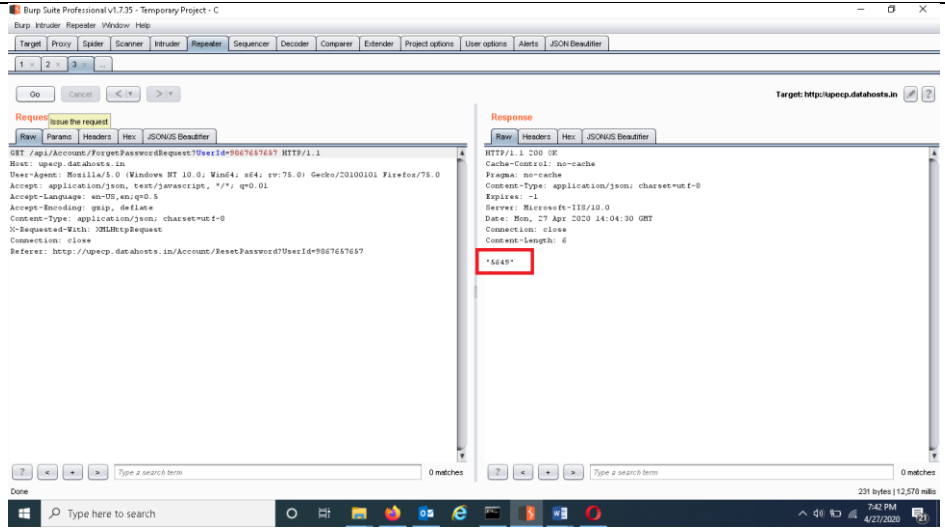



Web Application Compliance Security Audit Finding Report of

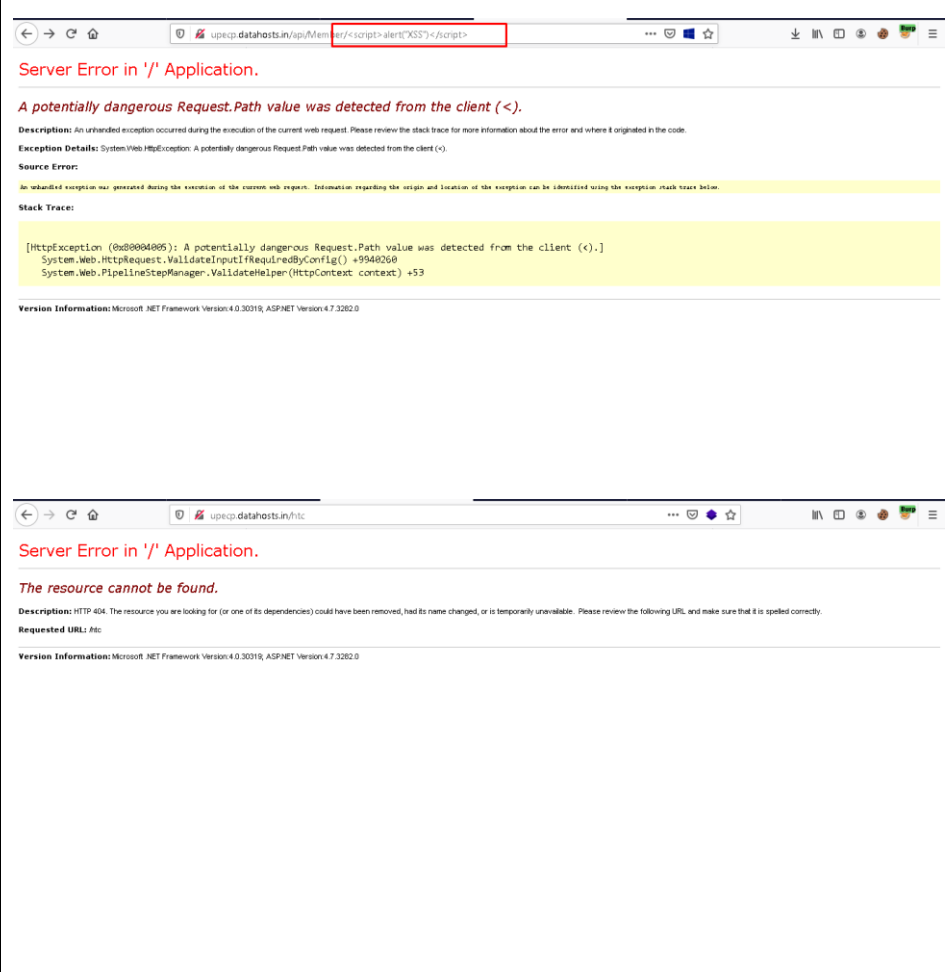
<http://upecp.datahosts.in/>

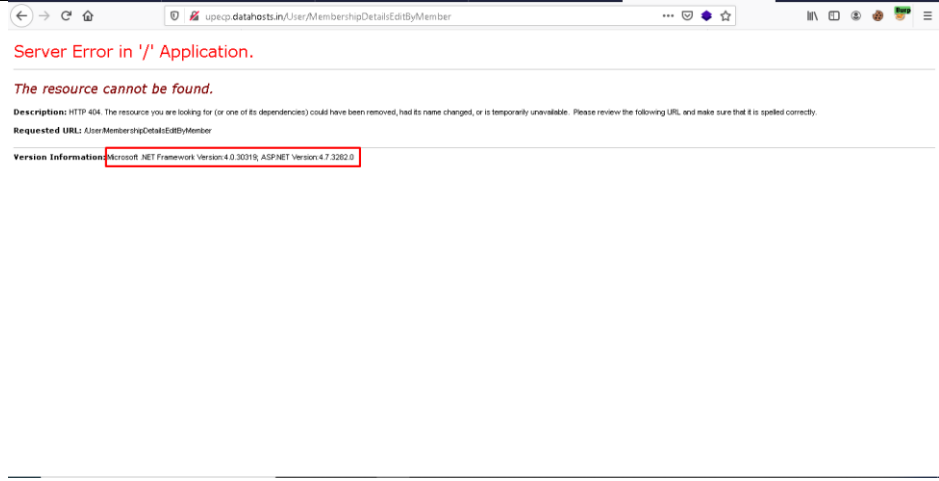
| 1) Vulnerability Title: File Upload | |
|-------------------------------------|---|
| Risk | High |
| Abstract | It was observed that the page contains functionality to handle file uploads and file management. |
| CVE | ----- |
| Ease of Exploitation | Easy |
| Impact | An attacker could use this functionality to upload double extension malicious executable files on the system to test file upload capabilities. |
| Recommendations | It is recommended to allow specific file format to upload the file and restrict Double extension files. |
| Snapshot |  <p>The screenshot shows a web application interface for editing membership details. It includes fields for IEC Code, GSTIN, EM-II, and Udyog Aadhaar. A red box highlights the file upload field where the file name 'test.jpg.exe' is entered. The interface also displays file upload requirements: 'File size must be less than 1024 KB. Only Pdf File Format'. Below the file upload field, there is a table for 'Please mention the articles being exported during the last two years together with value*'. The table has columns for S.No., Financial Years, Products, FOB Value (₹ in thousand), Countries of exports, and CA Certificate/Bank Certificate. The table contains one row with S.No. 1, Financial Years 2019-20, Products IT Products, FOB Value 1000000, Countries of exports American Samoa, American Samoa, Japan, Japan, and CA Certificate/Bank Certificate No file selected.</p> |
| Affected Site | http://upecp.datahosts.in/User/MembershipDetailsEditByMember |
| Compliance Status | Not Complied |

| 2) Vulnerability Title: OTP Flooding | |
|--------------------------------------|---|
| Risk | High |
| Abstract | It was observed that an attacker can flood a device with OTP messages on any mobile number which was required for registration |
| CVE | -- |
| Ease of Exploitation | Easy |
| Impact | An attacker can perform DoS (Denial of Services) attack on the Server as well as mobile device |
| Recommendations | It is recommended to restrict the number of SMS OTP sent to particular mobile number |
| Snapshot | NA |
| Affected Site | http://upecp.datahosts.in/Account/ResetPassword?UserId=9867657657 |
| Compliance Status | Complied |

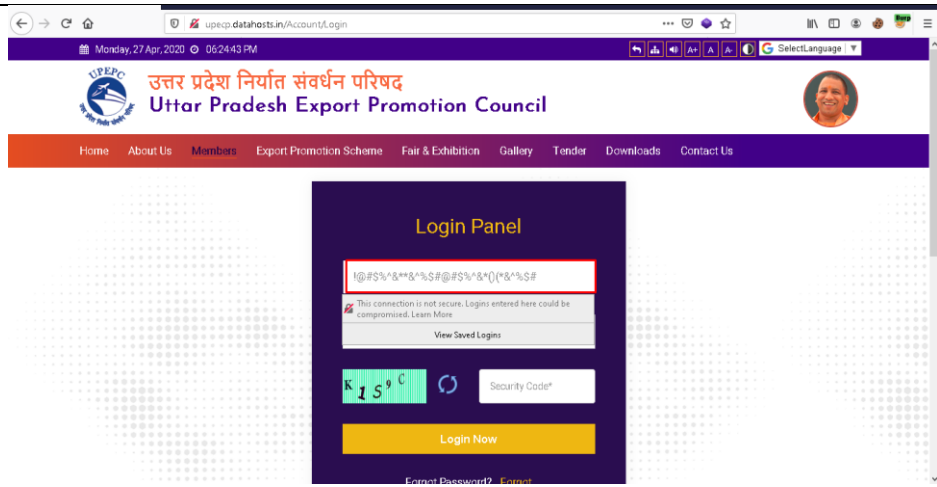
| 3) Vulnerability Title: OTP in Response | |
|---|--|
| Risk | High |
| Abstract | It was observed that an OTP is clear text in response |
| CVE | -- |
| Ease of Exploitation | Easy |
| Impact | An attacker can reset password and get unauthorized access to account. |
| Recommendations | It is recommended to OTP is masked or Hidden in response |
| Snapshot |  <p>The screenshot shows the Burp Suite Professional interface. The 'Response' tab is selected, displaying the raw HTTP response. The response body contains a JSON object with an 'otp' field, which has the value '5645'. This value is highlighted with a red rectangular box. The URL bar at the top shows the target URL: http://upecp.datahosts.in.</p> |
| Affected Site | http://upecp.datahosts.in/Account/ResetPassword?UserId=986765765 |
| Compliance Status | Complied |

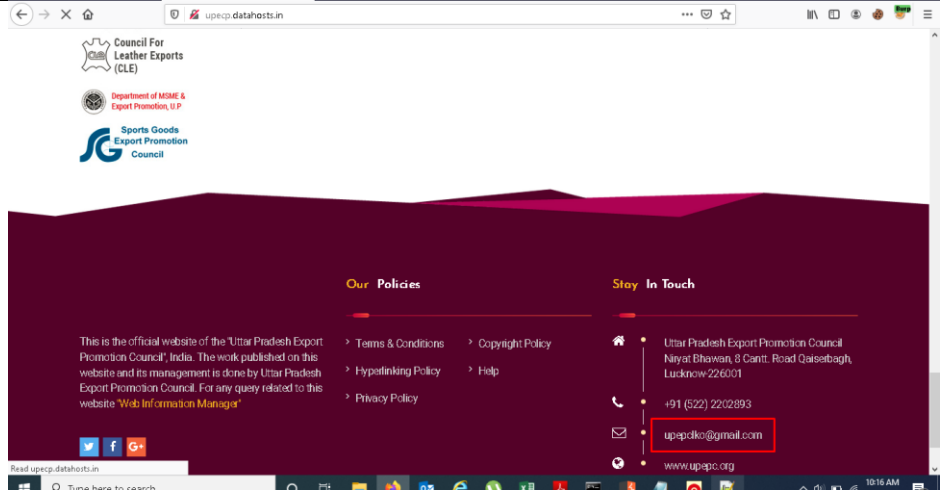
| 4) Vulnerability Title: Vulnerable JavaScript library | |
|---|--|
| Risk | Medium |
| Abstract | It was observed that a vulnerable Javascript Library found on the application. |
| CVE | ----- |
| Ease of Exploitation | Hard |
| Impact | XSS Vulnerability for applications with dynamic titles. http://bugs.jqueryui.com/ticket/6016 |
| Recommendations | It is recommends upgrade to the latest version. http://jquery.com/download/ |
| Snapshot |  |
| Affected Site | http://upecp.datahosts.in/Content/assets/js/jquery.min.js |
| Compliance Status | Not Complied |

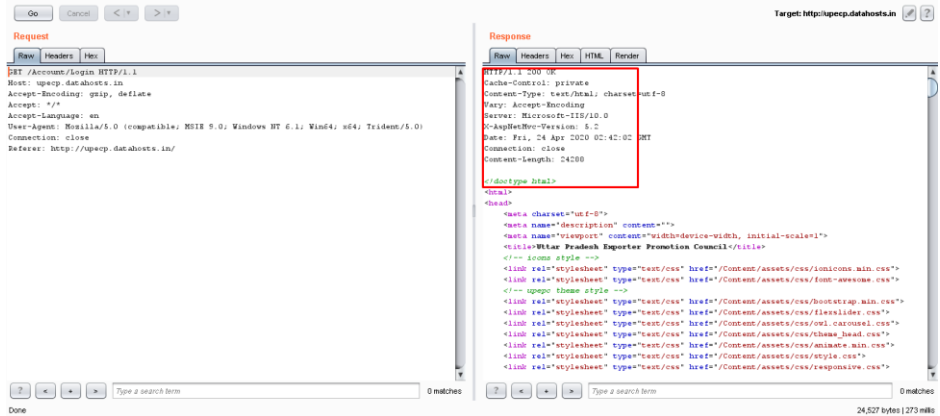
| 5) Vulnerability Title: Application Error | |
|---|--|
| Risk | Medium |
| Abstract | It was observed that there was vital information leakage on website. |
| CVE | ----- |
| Ease of Exploitation | Easy |
| Impact | It is possible to gather sensitive debugging information. |
| Recommendations | It is recommended to implement proper validations on URL input fields of the web application. |
| Snapshot |  <p>The first screenshot shows a 'Server Error in '/' Application.' message. The exception details indicate a 'potentially dangerous Request.Path value was detected from the client (<).' The stack trace shows the error originated in the 'System.Web.HttpRequest.ValidateInputIfRequiredByConfig()' method. The second screenshot shows a 'Server Error in '/' Application.' message with the description 'The resource cannot be found.' and the requested URL 'http://upecp.datahosts.in/htc'.</p> |
| Affected Site | http://upecp.datahosts.in/htc (All link) |
| Compliance Status | Complied |

| 6) Vulnerability Title: ASP.NET Version Disclosure | |
|--|---|
| Risk | Medium |
| Abstract | It was observed that there was vital information leakage on website. |
| CVE | ----- |
| Ease of Exploitation | Easy |
| Impact | The error message disclose sensitive information about ASP.NET version. This information can be used to launch further attacks. |
| Recommendations | <p>It is recommended to Set customErrors mode to Off or RemoteOnly. customErrors is part of system.web Element. RemoteOnly specifies that custom errors are shown only to the remote clients, and that ASP.NET errors are shown to the local host. This is the default value.</p> <pre><configuration> <system.web> <customErrors mode="RemoteOnly" /> </system.web> </configuration></pre> |
| Snapshot |  |
| Affected Site | http://upecp.datahosts.in/ * |
| Compliance Status | Not Complied |


| 7) Vulnerability Title: Session Timeout not implemented | |
|---|--|
| Risk | Medium |
| Abstract | It was observed that even if the Browser is logged in and idle it does not logout the session automatically |
| CVE | ----- |
| Ease of Exploitation | Medium |
| Impact | The lack of proper session expiration may improve the likelihood of certain session based attack where an attacker may intercept a session id possible via a network sniffer or cross site scripting attack. |
| Recommendations | It is recommended to implement account lockout. |
| Snapshot | N/A |
| Affected Site | http://upecp.datahosts.in/Admin/Index |
| Compliance Status | Complied |

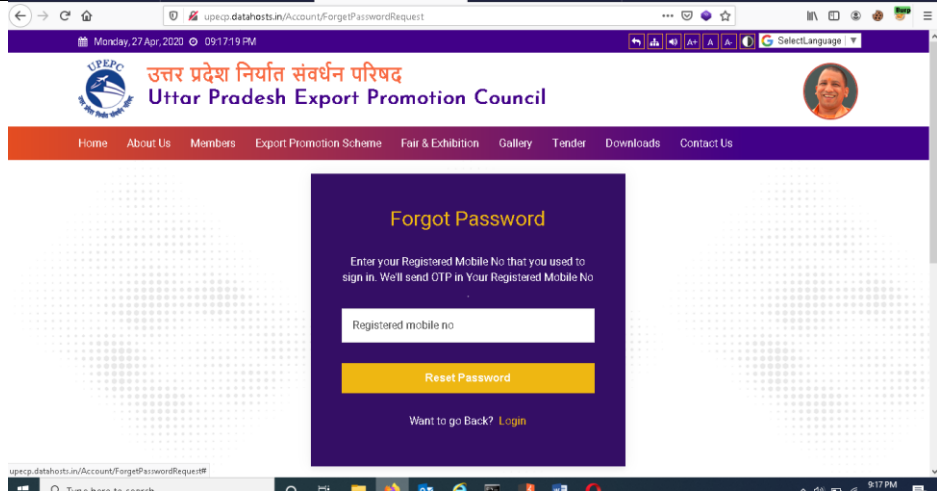
| 8) Vulnerability Title: input validation | |
|--|--|
| Risk | Low |
| Abstract | It was observed that there was vital information leakage on website. |
| CVE | ----- |
| Ease of Exploitation | Easy |
| Impact | An attacker can craft the input in a form that is not expected by the rest of the application. This will lead to parts of the system receiving unintended input, which may result in altered control flow, arbitrary control of a resource, or arbitrary code execution. |
| Recommendations | It is recommended to implement proper validations on all input fields of the web application. |
| Snapshot |  |
| Affected Site | http://upecp.datahosts.in/Account/Login (All-links) |
| Compliance Status | Not Complied |

| 9) Vulnerability Title: Email Address Found | |
|---|---|
| Risk | Low |
| Abstract | It was observed that the format of the email address found in the application was not set as per the best practice. |
| CVE | ----- |
| Ease of Exploitation | Easy |
| Impact | The spam bots (email harvesters and email extractors) are programs that scour the internet looking for email address on any website they come across. Spam bots looks for strings like myname@mydomain.com and then record any addresses found. |
| Recommendations | It is recommended that to replace @ with [at] and with [dot] or replace with image. |
| Snapshot |  <p>The screenshot shows the official website of the Uttar Pradesh Export Promotion Council. The header includes logos for the Council For Leather Exports (CLE), Department of MSME & Export Promotion, UP, and Sports Goods Export Promotion Council. The main content area features a dark blue background with a mountain silhouette. On the right side, under the 'Stay In Touch' section, the email address 'upcpdco@gmail.com' is listed and highlighted with a red rectangular box. Other contact information includes a phone number (+91 (522) 2202893) and a physical address in Lucknow.</p> |
| Affected Site | http://upecp.datahosts.in/ http://upecp.datahosts.in/home/firstofitskinds http://upecp.datahosts.in/home/galleryalbum |
| Compliance Status | Complied |

| 10) Vulnerability Title: HTTP Security Headers Not Implemented | |
|--|--|
| Risk | Low |
| Abstract | It was observed that security headers such as X-XSS protection, Content Security Policy, Strict Transport security policy, X-Content-Type-Options were not implemented in remote application. |
| CVE | ----- |
| Ease of Exploitation | Medium |
| Impact | If security headers are not implemented in application then it may help an attacker to exploit existing vulnerabilities in application logic and results in lack of defense in depth approach to prevent security attacks. |
| Recommendations | It is recommended to implement security headers to provide additional layer of security in application such as X-XSS protection, Content Security Policy, Strict Transport security policy, X-Content-Type-Options, |
| Snapshot |  <p>The screenshot displays the network traffic of a web browser. The 'Request' tab on the left shows a GET request to 'http://upecp.datahosts.in/'. The 'Response' tab on the right shows the server's reply with status '200 OK'. The response headers include 'Cache-Control: private', 'Content-Type: text/html; charset=utf-8', 'Vary: Accept-Encoding', 'Server: Microsoft-IIS/10.0', 'X-AppleNews-Version: 5.2', 'Date: Fri, 24 Apr 2020 02:42:02 ZST', 'Connection: close', and 'Content-Length: 24208'. The response body is HTML code starting with a meta charset declaration and several CSS links. The target URL 'http://upecp.datahosts.in' is visible in the browser's address bar.</p> |
| Affected Site | http://upecp.datahosts.in/ |
| Compliance Status | Not Complied |

| 11) Vulnerability Title: HTTP-OPTIONS Methods Enabled | |
|---|---|
| Risk | Low |
| Abstract | It was observed that Http options method is enabled on this web server. |
| CVE | CVE-2004-2320 |
| Ease of Exploitation | Easy |
| Impact | It was observed that using the Options method may expose sensitive information that may help a malicious user to prepare more advanced attacks |
| Recommendations | It is recommended to disable OPTIONS methods on the web server. |
| Snapshot | <p>The screenshot shows a web browser window with a 405 Method Not Allowed error. The request was a DELETE request to /api/Feedback/UpdateViewByAdmin?Mobile=904366491504. The response headers show 'Allow: GET, HEAD, OPTIONS, TRACE'. The response body contains an error message in Hindi: '405 - HTTP verb used to access this page is not allowed.'</p> |
| Affected Site | https://fulfilment-admin.azurewebsites.net/ |
| Compliance Status | Not Complied |

| 12) Vulnerability Title: X-Frame Option Header Missing | |
|--|---|
| Risk | Low |
| Abstract | It was observed that the X-Frame Option Header was missing. |
| CVE | ----- |
| Ease of Exploitation | Easy |
| Impact | An Attacker can conduct a Clickjacking Attack if the X-Frame option is not implemented |
| Recommendations | It is recommended that the application should return a response header with the name X-Frame-Options and the value DENY to prevent framing altogether, or the value SAMEORIGIN to allow framing only by pages on the same origin as the response itself. |
| Snapshot |  <p>The screenshot shows a web browser window with a warning message at the top: "Website is vulnerable to clickjacking!". Below the warning, a frame displays the Uttar Pradesh Export Promotion Council website. The website has a purple header with the council's name in Hindi and English. The main content area has a white background with a purple sidebar. The text on the page reads: "Welcome to Uttar Pradesh Export Promotion Council. Uttar Pradesh, India's fifth largest and the most populous state has always been in the forefront in the area of industrial development. The state has the status of 3rd largest economy of the country and has achieved remarkable growth in exports during last few years. As of 2018-19 export data Uttar Pradesh stood 5th in the Country in exports."</p> |
| Affected Site | http://upecp.datahosts.in/ |
| Compliance Status | Not Complied |

| 13) Vulnerability Title: CAPTCHA Not Implemented | |
|--|--|
| Risk | Low |
| Abstract | It was observed that there was no captcha implemented on the given web application forms. |
| CVE | ----- |
| Ease of Exploitation | Medium |
| Impact | An attacker can brute force at input forms (with dummy data) which could lead to increase in logs or database entries on the server. |
| Recommendations | It is recommended to implement captcha at web forms. |
| Snapshot |  |
| Affected Site | http://upecp.datahosts.in/Account/ForgetPasswordRequest |
| Compliance Status | Not Complied |

New Findings:

| 14) Vulnerability Title: Cross-Site Request Forgery | |
|---|---|
| Risk | High |
| Abstract | Insufficient integrity verification method was used by the application. |
| CVE | ----- |
| Ease of Exploitation | Easy |
| Impact | It is possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user |
| Recommendations | <p>"In order to avoid CSRF attacks, every request should contain a unique identifier, which is a parameter that an attacker cannot guess. One suggested option is to add the session id taken from the session cookie and adding it as a parameter. The server must check that this parameter matches the session cookie, and if not discard the request. The reason an attacker cannot guess this parameter is the ""same origin policy"" that applies to cookies, so the attacker cannot forge a fake request that will seem real to the server.</p> <p>Any secret that is hard to guess and is not accessible to an attacker (i.e. not accessible from a different domain) can be used instead of the session id.</p> <p>This will prevent an attacker from crafting a seemingly valid request.</p> <p>"</p> |

Snapshot

upecp.datahosts.in/Admin/ApproveMemberRequestList

Penetration Testing... Dashboard

Date From: Date To: Mobile No: -Select District: Select ExporterType: Q Search

Show: 100 entries

| S.No. | District | Member Id | Name of Firm | IEC Code | Exporter Type | Mobile No. | Certificate downloaded by member | Status | Registration Status | Action |
|-------|-----------|--------------------------|--------------|------------|---------------------------|------------|----------------------------------|----------|---------------------|--------|
| 1 | Agra | UPEPC-0102031518/2020-21 | test company | 0508011395 | Manufacturer cum Merchant | 9918578212 | No | Approved | Active | |
| 2 | Aligarh | UPEPC-0201041517/2020-21 | DFGDFG | 6789 | Prospective Exporter | 9875984375 | No | Approved | Active | |
| 3 | Prayagraj | UPEPC-0302041516/2020-21 | tttttt | oooooooo | Prospective Exporter | 7777777777 | No | Approved | Active | |
| 4 | Prayagraj | UPEPC-0303041515/2020-21 | tttttt | uuuuuuuu | Prospective Exporter | 8888888888 | No | Approved | Active | |
| 5 | Azamgarh | UPEPC- | test | RRRRRRRR | Manufacturer cum | 9876543210 | No | Approved | Active | |

upecp.datahosts.in/Admin/EditMembershipDetailByAdmin?id=UPEPC-0102030002/2020-21

Go Cancel < >

Request

Raw Params Headers Hex

POST /api/Member/UpdateMemberDetailsByAdmin HTTP/1.1
Host: upecp.datahosts.in
Content-Length: 7456
Accept: */*
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.97 Safari/537.36
Content-Type: multipart/form-data; boundary=----WebkitFormBoundaryCnagmD8CUTVAeM4
Origin: http://upecp.datahosts.in

Response

Raw Headers Hex

HTTP/1.1 200 OK
Cache-Control: no-cache
Pragma: no-cache
Content-Type: application/json; charset=utf-8
Expires: -1
Server:
Date: Wed, 17 Jun 2020 09:32:18 GMT
Content-Length: 155
Content-Type: close

["ResultStatus": "s", "ResultMessage": "Successfully Updated.", "MobileNo": "9918578212", "FlagForExistingMember": null, "ResultMessage": "Congratulation! Member information is successfully updated."]

Done

upecp.datahosts.in/Admin/EditMembershipDetailByAdmin?id=UPEPC-0102030002/2020-21

Penetration Testing... Dashboard

Name of Proprietor/All Directors/ Partners*

| S.No. | Name | Designation | Mobile no | Email | |
|-------|---------------|-------------|------------|--------------|--|
| 1 | sumit agarwal | Proprietor | 9918578212 | care@ptpl.in | |
| 2 | nishat | | | dd@dd.com | |

Person(s) who shall exercise the rights and

| S.No. | Name | |
|-------|-----------|--|
| 1 | test tte | |
| 2 | asdfsadfa | |

any variation here in from time to time*

| S.No. | Email | |
|-------|----------------|--|
| 1 | sdfsdfs@dd.com | |

Update

Success!

Congratulation! Member information is successfully updated.

OK

Affected Site

<http://upecp.datahosts.in/Admin/Index>(All-links)

| 15) Vulnerability Title: Cross Site Scripting(DOM-BASED)&(Reflected) | |
|--|--|
| Risk | High |
| Abstract | <p>It was observed that</p> <p>The application may be vulnerable to DOM-based cross-site scripting. Data is read from window.location.pathname and passed to \$() via the following statements:</p> <pre>var currurl = window.location.pathname; \$('li:has(a[href="'+ currurl + '"])').addClass('active');</pre> |
| CVE | ----- |
| Ease of Exploitation | Hard |
| Impact | Malicious users may inject JavaScript, VBScript, ActiveX, HTML or Flash into a vulnerable application to fool a user in order to gather data from them. An attacker can steal the session cookie and take over the account, impersonating the user. |
| Recommendations | <p>It is recommended that The most effective way to avoid DOM-based cross-site scripting vulnerabilities is not to dynamically write data from any untrusted source into the HTML document and necessary to sanitize or encode the data. to</p> <p>filter out all the following characters at user input:</p> <ul style="list-style-type: none"> [1] (pipe sign) [2] & (ampersand sign) [3] ; (semicolon sign) [4] \$ (dollar sign) [5] % (percent sign) [6] @ (at sign) [7] ' (single apostrophe) [8] " (quotation mark) [9] \' (backslash-escaped apostrophe) [10] \" (backslash-escaped quotation mark) [11] <> (triangular parenthesis) [12] () (parenthesis) [13] + (plus sign) [14] CR (Carriage return, ASCII 0x0d) [15] LF (Line feed, ASCII 0x0a) [16] , (comma sign) [17] \ (backslash) |

Snapshot

The screenshot displays a web browser window with two tabs. The active tab is titled "view-source:upecp.datahosts.in" and shows a JavaScript source file. The code includes several functions and event listeners. A red box highlights a specific line of code: `var currurl = window.location.pathname;`. The second tab is titled "upecp.datahosts.in/Admin/EditMembershipDetailByAdmin?AdminId=UPEPC-0201040003/2020-21" and shows a web application interface. The interface includes a "Choose File" button, a "Click here View File" link, and a form with a table of members. An error message is displayed in the center of the screen, stating: "Error: Conversion failed when converting the varchar value 'POST /api/Member/UpdateMemberDetailsByAdmin HTTP/1.1' to data type bit." The error message is highlighted with a red box.

```
document.write("<script type='text/javascript' src='/App35/FrontIndexList.js?v=" + Date.now() + "></script>");
document.write("<script type='text/javascript' src='/App35/FrontIndexGallery.js?v=" + Date.now() + "></script>");

</script>

<script>
$('aapply').click(function () {
    location.href = "/Home/MembershipDetail"
});
</script>

<script>
$(function () {
    $(document).on('focus', ':input', function () {
        $(this).attr('autocomplete', 'off');
    });
    $('aLink').removeClass('active');
    var currurl = window.location.pathname;
    if ($('aLink').has('href' + currurl + ".html").length) {
        $('aLink').addClass('active');
    }
    //document.addEventListener('contextmenu', function (e) {
    //    e.preventDefault();
    //});
    document.onkeypress = function (event) {
        event = (event || window.event);
        if (event.keyCode == 123) {
            return false;
        }
    }
    document.onmousedown = function (event) {
        event = (event || window.event);
        if (event.keyCode == 123) {
            return false;
        }
    }
    document.onkeydown = function (event) {
        event = (event || window.event);
        if (event.keyCode == 123) {
            return false;
        }
    }
});
</script>
```

Activate Windows
Go to Settings to activate Windows.

Choose File | No file chosen | Choose File | Software List - Copy.exe.pdf

Click here View File

Whether member of any other Export Promotion Council.(Yes/No)
☐ Yes ☒ No

Name of Proprietor/All Directors/ Partners

| S.No. | Name |
|-------|----------|
| 1 | DFHGGGFH |

Person(s) who shall exercise the rights and

| S.No. | Name |
|-------|------|
| 1 | HJK |

Email

| Email |
|-----------|
| GG@DF.HJK |
| G@FF.HJK |

any variation here in from time to time"

Update

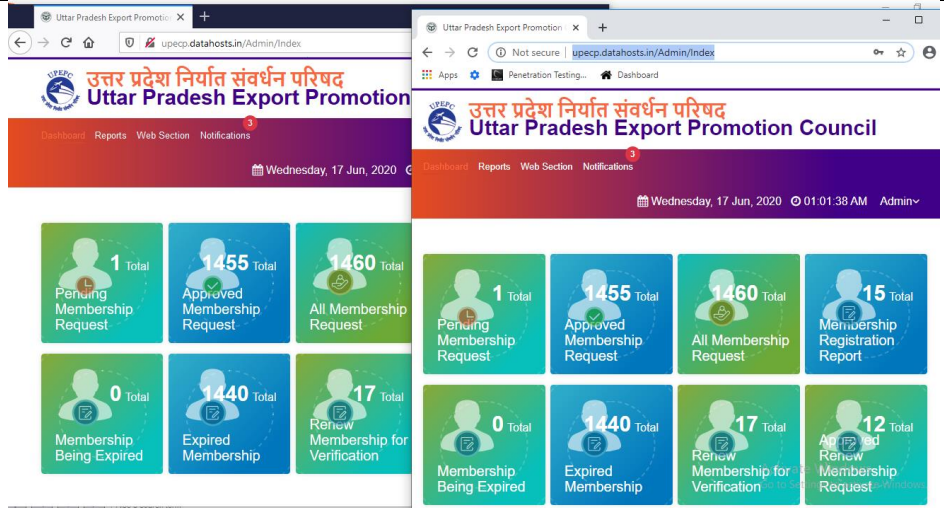
Error

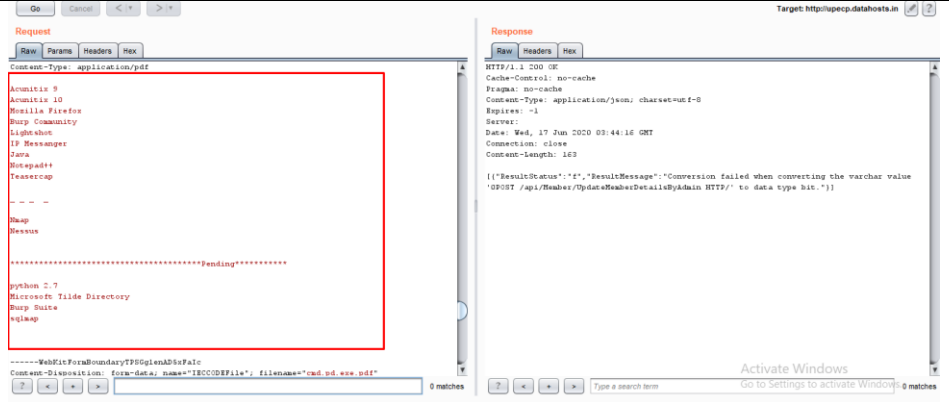
Conversion failed when converting the varchar value 'POST /api/Member/UpdateMemberDetailsByAdmin HTTP/1.1' to data type bit

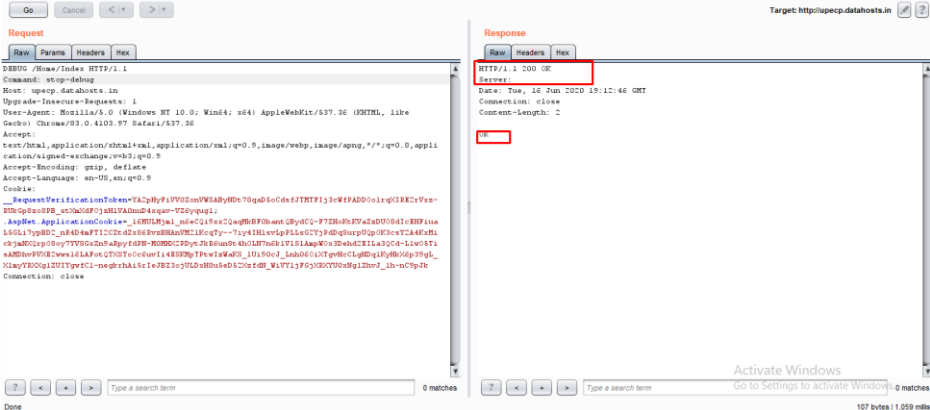
OK

Affected Site

<http://upecp.datahosts.in/> (All-links)

| 16) Vulnerability Title: Multiple Browser Login of Admin at the same | |
|--|---|
| Risk | Medium |
| Abstract | It is observed that the same user can login into via multiple browsers. |
| CVE | ----- |
| Ease of Exploitation | Medium |
| Impact | The attacker can use the same login ID for exploitation even if the ID is active. |
| Recommendations | It is recommended to restrict multiple browser login for admin at the same time. |
| Snapshot |  |
| Affected Site | http://upecp.datahosts.in/Admin/Index |

| 17) Vulnerability Title: Data Disclosure on attached files | |
|--|--|
| Risk | Medium |
| Abstract | It was observed that the Data in the attached in the Application is traveling over an Unencrypted Communication channel and is disclosed in the request |
| CVE | ----- |
| Ease of Exploitation | Easy |
| Impact | A user can view a list of all files from this documents which can lead to sensitive information disclosure and proceed attacks using those data. |
| Recommendations | It is recommended to attached files travel over an Encrypted Channel and those Data are not disclosed to the User. |
| Snapshot |  <p>The screenshot shows a web browser window with the target URL http://upecp.datahosts.in. The browser displays a request and response. The request is a GET request to the target URL. The response is a 200 OK status with a Content-Type of application/pdf. The response body contains a list of files: Acrobat 5, Acrobat 10, Mozilla Firefox, Sharp Community, Lightshot, IP Messenger, Java, Winpad++, Teasecap, and a list of files: python 2.7, Microsoft Tilde Directory, Sharp Suite, and vglap.</p> |
| Affected Site | http://upecp.datahosts.in/User/MembershipDetailsEditByMember http://upecp.datahosts.in/Admin/Index |

| 18) Vulnerability Title: ASP.NET debugging enabled | |
|--|---|
| Risk | Low |
| Abstract | It was observed that .net debugging mode was enabled on given application. |
| CVE | ----- |
| Ease of Exploitation | Medium |
| Impact | It may be possible to disclose sensitive information about the web sever the ASP.NET application. |
| Recommendations | It is recommended to disable debug mode for this application by setting debug=false in the Web.config file for each application on the server |
| Snapshot |  |
| Affected Site | http://upecp.datahosts.in/ |